



Functional Bureau Strategy

Bureau of Cyberspace and Digital Policy

FOR PUBLIC RELEASE

Approved: June 9, 2023

Table of Contents

1. Executive Statement and Mission Statement..... 3

2. Bureau Strategic Framework 5

3. Bureau Goals and Objectives 7

4. Bureau Cross-Cutting Management Goal 17

1. Executive Statement and Mission Statement

Mission Statement: The Bureau of Cyberspace and Digital Policy (CDP) promotes U.S. national and economic security by leading, coordinating, and elevating foreign policy on cyberspace and digital technologies. It builds partnerships to shape the international environment so Americans and people everywhere can prosper. CDP strives for a world in which every person can access the opportunities that come with digital connectivity to build thriving economies and societies and works to counter challenges to this vision from authoritarian states.

Technology is a source of national power. Nearly all foreign policy issues – from arms control to democracy and human rights to global health and climate change – will be shaped by today’s investments in cyber, digital, and emerging technology diplomacy. Gains in this space offer broad societal benefits. Guided by the appropriate standards and norms, and grounded in democratic values, technological innovation will improve lives around the world and help address shared global challenges.

The stakes for international technology diplomacy are high. From free markets to the rule of law to equal treatment for all people, U.S. and democratic values will succeed only if rights-respecting countries prevail in the competitions now being waged over the development, deployment, and use of critical and emerging technologies. Common understandings of trust, interoperable standards, and shared norms and values can only be developed by working closely with partners and allies.

Recognizing the growing role of technology as a cross-cutting national security issue, the Department created CDP in April 2022 to lead and coordinate U.S. diplomacy on cyber and digital policy. The bureau addresses the national security challenges and economic opportunities presented by cyberspace and digital technologies and promotes standards and norms that are fair, transparent, and support the rights-respecting use of technology. Through robust engagement in multilateral organizations and with the multistakeholder community, bilateral diplomacy with partners round the world, and encouragement of responsible and rights-respecting state behavior in cyberspace, CDP empowers U.S. leadership in cyber, digital, and technology diplomacy.

Approved: June 9, 2023

As citizens around the world eagerly seek increased internet connectivity to harness the tremendous opportunities afforded by the digital transformation, CDP leads, coordinates, and implements foreign assistance programs designed to ensure connectivity is secure, meaningful, governed fairly, and first and foremost serves the interests of its users. Through diplomacy, international cooperation, foreign assistance, and deterrence, the United States continues to advance an affirmative positive vision of technology as a tool that supports that promotes collective security, prosperity, and democratic values while discrediting authoritarian alternatives.

2. Bureau Strategic Framework

Bureau Goal 1: Advance cyber and digital policies that align with U.S. national interests and foreign policy objectives.

- **Bureau Objective 1.1:** Bilateral diplomacy: Deepen relationships with existing U.S. partners, forge new partnerships, and engage with a range of countries to advance a common vision for the Internet and digital technologies.
- **Bureau Objective 1.2:** Multilateral diplomacy: Leverage key multilateral fora to build relationships, advance U.S. policy priorities, and guard against positions that are counter to U.S. approaches to the Internet and digital technologies.
- **Bureau Objective 1.3:** External stakeholders: Identify, enhance, cultivate, and develop strategic engagements across the private sector and multistakeholder communities.
- **Bureau Objective 1.4:** Capacity Building: Increase secure and open digital connectivity and access to the Internet.
- **Bureau Objective 1.5:** Public diplomacy: Implement public messaging and public diplomacy programs to expand key audiences' understanding and support of U.S. cyber and digital policies.

Bureau Goal 2: Integrate and elevate U.S. cyberspace and digital foreign policy through robust communication and collaboration with other elements of the Department and Interagency.

- **Bureau Objective 2.1:** Integrate cyberspace and digital policy knowledge, skills, and strategies throughout the Department of State.
- **Bureau Objective 2.2:** Elevate the State Department's role within the Interagency to develop and implement U.S. cyberspace and digital foreign policy, assistance, and messaging.

Bureau Cross-Cutting Management Goal 1: Create a positive, career-enhancing place to work, with clear processes and a cohesive bureau culture that values innovation and collaboration.

- **Bureau Cross-Cutting Management Objective 1.1:** Hire, develop and retain a diverse and highly qualified workforce.
- **Bureau Cross-Cutting Management Objective 1.2:** Establish, implement, and strengthen CDP processes and systems to maximize effectiveness and efficiency.
- **Bureau Cross-Cutting Management Objective 1.3:** Cultivate a bureau culture grounded in diversity, equity, inclusion, accessibility, collaboration, and innovation.

3. Bureau Goals and Objectives

Bureau Goal 1: Advance cyber and digital policies that align with U.S. national interests and foreign policy objectives.

- **Bureau Goal 1 Description:** Technology plays a critical role in empowering people to achieve their greatest ambitions and potential. We envision a future where people around the world use digital technologies securely to safely and openly engage online. In the digital age, this approach allows governments to share valuable information and provide critical services to their citizens. It is how people everywhere communicate, innovate, and prosper, driving economic growth. CDP will advance programs and policies that help achieve our goals and reflect our values, including inclusive economic prosperity; responsive and rights-respecting democracy; and a vibrant and diverse society.

Just as democracies are evolving to address the challenges of the 21st century, technology must evolve too. An open, interoperable, secure, and reliable Internet enables new solutions to key policy objectives, including addressing climate change, reducing food insecurity, improving global public health, meeting the Sustainable Development Goals, and promoting democratic renewal.

CDP promotes its vision for the digital technologies and a stable cyberspace through bilateral and multilateral diplomacy with foreign governments, including capacity building, and engagement with non-government stakeholders. CDP prioritizes three lines of effort: 1) maintaining international cyberspace security through policies and activities that uphold the framework of responsible state behavior in cyberspace and deter bad actors, and support U.S. cyber operations; 2) promoting secure and trusted telecommunications services and infrastructure, encouraging cross-border data flows, and advocating for multistakeholder approaches to Internet and digital technology governance; and 3) promoting digital freedoms through policies and activities that are rights enabling and rights protecting. These efforts will expand the benefits of the

digital world while maintaining stability in cyberspace and addressing harmful uses of digital technologies.

Bureau Objective 1.1: Bilateral diplomacy: Deepen relationships with existing U.S. partners, forge new partnerships, and engage with a range of countries to advance a common vision for the Internet and digital technologies.

- **Bureau Objective 1.1 Justification and Linkages:** The United States must engage bilaterally to build and strengthen partnerships with likeminded governments to meet our shared objectives through cooperation and coordination. In addition, CDP must look to build bilateral ties and agreements with nations that have been historically less aligned with the United States to expand international likeminded coalitions. Strengthening and expanding coalitions in support of an affirmative vision for cyberspace is essential to ensure innovative ecosystems and rights-respecting digital technologies and policies persist.

This objective links to the NSS and its specific components on shaping the rules of the road, the use of technology, and securing cyberspace, as well as the 2023 National Cybersecurity Strategy. It also aligns with JSP Strategic Objective 2.3: “Support U.S. technological leadership, strengthen competitiveness, and enhance and protect the U.S. innovation base while leveraging technology to improve lives around the world”. This objective contributes to JSP Goal Statement 1.4.2 to “promote a Stable Cyberspace by September 30, 2026, sustain and enhance international cooperation to promote the U.S. vision of an open, interoperable, reliable, and secure internet and a stable cyberspace; and strengthen the capacity of the United States and partner nations to detect, deter, mitigate, and respond to international cyber threats and incidents.”

- **Bureau Objective 1.1 Risk Considerations:** Partners will likely continue to experience major cyber incidents in the coming years, testing our ability to respond quickly and effectively. These incidents could result in breaches of sensitive information or disruptions to critical infrastructure. Meanwhile, new partners may seek greater financial support for connectivity infrastructure and cybersecurity tools than the United

States and its partners are currently equipped to provide. To mitigate these risks, CDP will build trust and deepen relationships with foreign partner governments and stakeholder communities through open communication, transparency, and a commitment to an affirmative vision for cyberspace and global connectivity that reflects our values and supports shared prosperity. CDP will also build and strengthen international coalitions and work to increase the number of countries aligned with U.S. positions.

Bureau Objective 1.2: Multilateral diplomacy: Leverage key multilateral fora to build relationships, advance U.S. policy priorities, and guard against positions that are counter to U.S. approaches to the Internet and digital technologies.

- **Bureau Objective 1.2 Justification and Linkages:** CDP must engage in diplomatic efforts to promote multilateral cooperation and dialogue on cyber and digital issues, including by participating in international forums and working groups, such as the regional security organizations (i.e., OAS, OSCE, ARF), Internet Governance Forum, First and Third Committees of the UN General Assembly, the Organization for Economic and Cooperation and Development, the G7, G20, and the International Telecommunication Union, to promote the adoption of common principles and norms of responsible state behavior with the use of digital technologies. CDP will coordinate with USAID on its multilateral partnerships and investments focused on Digital Development.

This objective links to the NSS and its specific components on shaping the rules of the road, the use of technology, and securing cyberspace, as well as the 2023 National Cybersecurity Strategy. It also aligns with JSP Strategic Objective 2.3: “Support U.S. technological leadership, strengthen competitiveness, and enhance and protect the U.S. innovation base while leveraging technology to improve lives around the world”. This objective contributes to JSP Goal Statement 1.4.2 to “promote a Stable Cyberspace by September 30, 2026, sustain and enhance international cooperation to promote the U.S. vision of an open, interoperable, reliable, and secure internet and a stable cyberspace;

and strengthen the capacity of the United States and partner nations to detect, deter, mitigate, and respond to international cyber threats and incidents.”

- **Bureau Objective 1.2 Risk Considerations:** The risks associated with this objective include competing priorities within each multilateral forum, a proliferation of forums with overlapping agendas, and the need to continue strong advocacy for U.S. interests. To mitigate these risks, CDP will establish clear policy priorities, which it will map to the various organizations. CDP will foster collaboration and information sharing with other nations and organizations to help build trust and advance common interests. In addition, CDP will encourage and support partner participation in multilateral fora.

Bureau Objective 1.3: External stakeholders: Identify, enhance, cultivate, and develop strategic engagements across the private sector and multistakeholder communities.

- **Bureau Objective 1.3 Justification and Linkages:** CDP will encourage engagement with the multistakeholder community to advance a common vision for the Internet and digital technologies, including by partnering with businesses and industry groups to promote responsible and ethical practices around the use of digital technologies and to support the development of innovation and entrepreneurship in emerging economies.

This objective links to the NSS and its specific components on shaping the rules of the road, the use of technology, and securing cyberspace, as well as the 2023 National Cybersecurity Strategy. It also aligns with JSP Strategic Objective 2.3: “Support U.S. technological leadership, strengthen competitiveness, and enhance and protect the U.S. innovation base while leveraging technology to improve lives around the world”. This objective contributes to JSP Goal Statement 1.4.2 to “promote a Stable Cyberspace by September 30, 2026, sustain and enhance international cooperation to promote the U.S. vision of an open, interoperable, reliable, and secure internet and a stable cyberspace; and strengthen the capacity of the United States and partner nations to detect, deter, mitigate, and respond to international cyber threats and incidents.”

- **Bureau Objective 1.3 Risk Considerations:** The risks associated with this objective include potential conflicts of interest between the public and private sectors, a perception of favoritism, balancing security with privacy and other human-rights grounded values, and management of information sharing and confidentiality. To mitigate these risks, CDP will develop detailed plans that establish clear objectives for partnerships that align with U.S. interests and values.

Bureau Objective 1.4: Capacity Building: Increase secure and open digital connectivity and access to the Internet.

- **Bureau Objective 1.4 Justification and Linkages:** CDP will work to increase access to an open, interoperable, secure, and reliable Internet. Trusted digital connectivity is essential for economic growth and competitiveness, and expanding meaningful access can lead to a more equitable and inclusive society. Cybersecurity best practices and cyberspace policies are essential to realize the benefits of digital technologies and prevent their misuse. By leveraging a history of strong programming on digital and cyber issues, coordinating with other functional and regional bureaus with track records of highly effective cyber and tech-related programs, and integrating digital freedom policies into foreign assistance programs, CDP will strengthen the impact of its capacity building efforts.

This objective links to the NSS and its specific components on shaping the rules of the road, the use of technology, and securing cyberspace, as well as the 2023 National Cybersecurity Strategy. It also aligns with JSP Strategic Objective 2.3: “Support U.S. technological leadership, strengthen competitiveness, and enhance and protect the U.S. innovation base while leveraging technology to improve lives around the world”. This objective contributes to JSP Goal Statement 1.4.2 to “promote a Stable Cyberspace by September 30, 2026, sustain and enhance international cooperation to promote the U.S. vision of an open, interoperable, reliable, and secure internet and a stable cyberspace; and strengthen the capacity of the United States and partner nations to detect, deter, mitigate, and respond to international cyber threats and incidents.”

- **Bureau Objective 1.4 Risk Considerations:** The risks associated with achieving this objective include the potential that partners' needs outstrip the available funding resources and/or the required expertise or solutions cannot be efficiently leveraged. To mitigate these risks, CDP will take steps to prioritize foreign assistance, strengthen partnerships with the private sector and likeminded international partners, and encourage the growth of a community of relevant capacity building implementers. In addition, CDP will work with other bureaus and the Interagency to bring funding and expertise to bear in CDP's capacity building programs.

Bureau Objective 1.5: Public diplomacy: Implement public messaging and public diplomacy programs to expand key audiences' understanding and support of U.S. cyber and digital policies.

- **Bureau Objective 1.5 Justification and Linkages:** Because tailored messaging programs can increase understanding and support of U.S. cyber and digital policies, CDP will adopt an approach that enhances the effectiveness of outreach efforts. CDP policymakers can also solicit direct feedback through direct engagement with audiences. By openly communicating our policies and initiatives, CDP can demonstrate its commitment to transparency, an affirmative U.S. vision for the Internet and digital technologies, and the promotion of a secure and stable cyberspace and digital ecosystem.

This objective links to the NSS and its specific components on shaping the rules of the road, the use of technology, and securing cyberspace, as well as the 2022 National Cybersecurity Strategy. It also aligns with JSP Strategic Objective 2.3: "Support U.S. technological leadership, strengthen competitiveness, and enhance and protect the U.S. innovation base while leveraging technology to improve lives around the world". It supports JSP Objective 1.5: Enhance foreign publics' understanding of and support for the values and policies of the United States.

- **Bureau Objective 1.5 Risk Considerations:** The risks associated with this objective include the potential for misinformation and disinformation to undermine U.S. messaging efforts. To mitigate these risks, CDP will track misinformation and disinformation related to U.S. cyber and digital policy and proactively message with targeted and strategic audiences to ensure that messaging about U.S. cyber and digital policies is accurate, transparent, and focused on building trust and credibility with audiences. CDP will also expand public diplomacy programs that build medium and long-term partnerships with key stakeholders via exchange programs and other professional development opportunities, aiming to cultivate enduring trust among opinion leaders around the world working at the intersection of technology and foreign policy.

Bureau Goal 2: Integrate and elevate U.S. cyberspace and digital foreign policy through robust communication and collaboration with other elements of the Department and Interagency.

- **Bureau Goal 2 Description:** As a new bureau at the Department of State with a mandate to coordinate U.S. diplomacy on cyberspace and digital policy, it is critical that CDP promote and coordinate these issues across the Department and the interagency. To succeed, CDP must engage and upskill staff across the Department. In addition, CDP must elevate the Department's role in the Interagency to develop and implement U.S. cyberspace and digital foreign policy, assistance, and messaging. CDP will look to strengthen coordination with USAID in the areas of digital development and diplomacy while also seeking to foster interagency collaboration by developing clear lines of communication and coordination across different agencies and departments involved in U.S. cyber and digital policy. It will promote information sharing and the coordination of foreign policy efforts.

Bureau Objective 2.1: Integrate cyberspace and digital policy knowledge, skills, and strategies throughout the Department of State.

- **Bureau Objective 2.1 Justification and Linkages:** Fully integrating cyberspace and digital policy knowledge, skills, and strategies into U.S foreign policy is critical for addressing the complex and rapidly evolving challenges of the digital age. CDP will develop a comprehensive training program for U.S. diplomats that includes the technical and policy-related aspects of cyberspace and digital policy. This program will be strongly encouraged for employees working on these issues and will include regular updates to keep pace with technological and policy changes. CDP will also champion regular collaboration and information-sharing among different stakeholder offices and functional and regional bureaus to ensure that expertise is shared throughout the organization.

This objective links to the NSS and its specific components on shaping the rules of the road, the use of technology, and securing cyberspace, as well as the 2022 National Cybersecurity Strategy. It also aligns with JSP Strategic Objective 2.3: “Support U.S. technological leadership, strengthen competitiveness, and enhance and protect the U.S. innovation base while leveraging technology to improve lives around the world”. This objective contributes to JSP Goal Statement 1.4.2 to “promote a Stable Cyberspace by September 30, 2026, sustain and enhance international cooperation to promote the U.S. vision of an open, interoperable, reliable, and secure internet and a stable cyberspace; and strengthen the capacity of the United States and partner nations to detect, deter, mitigate, and respond to international cyber threats and incidents.”

- **Bureau Objective 2.1 Risk Considerations:** The risks associated with achieving this objective include the potential for silos, communication gaps, missed coordination opportunities among the various impacted parties, as well as a lack of capacity to effectively train and equip our workforce. To mitigate these risks, CDP will work closely with FSI and others to develop training and education opportunities that build the capabilities of cyber and digital economy officers. It will coordinate closely with regional and functional bureaus to integrate cyber and digital policy priorities into their work and

strategic plans. It will also work with Department leadership to further explore ways to institutionalize incentives for those working on tech diplomacy across the organization.

Bureau Objective 2.2: Elevate the State Department's role within the Interagency to develop and implement U.S. cyberspace and digital foreign policy, assistance, and messaging.

- **Bureau Objective 2.2 Justification and Linkages:** A more prominent role for the State Department within the Interagency in developing and implementing U.S. cyberspace and digital foreign policy, assistance, and messaging will better advance U.S. interests and protect national security in the digital age. Congress and the White House have recognized this key role by assigning responsibility to the State Department (and specifically to CDP) for the development of a clear and comprehensive U.S. International Cyberspace and Digital Policy strategy to be developed in consultation with other agencies.

CDP will work to strengthen collaboration with other agencies involved in cyberspace and digital policy, including the U.S. Agency for International Development, Department of Defense, Intelligence Community, Department of Justice, and Department of Homeland Security. It will also work to lead the development of coordinated messaging on cyberspace and digital policy. This will include collaboration with other agencies to develop key messages, talking points, and communication strategies.

This objective links to the NSS and its specific components on shaping the rules of the road, the use of technology, and securing cyberspace, as well as the 2022 National Cybersecurity Strategy. It also aligns with JSP Strategic Objective 2.3: "Support U.S. technological leadership, strengthen competitiveness, and enhance and protect the U.S. innovation base while leveraging technology to improve lives around the world". This objective contributes to JSP Goal Statement 1.4.2 to "promote a Stable Cyberspace by September 30, 2026, sustain and enhance international cooperation to promote the U.S. vision of an open, interoperable, reliable, and secure internet and a stable cyberspace; and strengthen the capacity of the United States and partner nations to detect, deter, mitigate, and respond to international cyber threats and incidents."

- **Bureau Objective 2.2 Risk Considerations:** The risks associated with this objective include cooperation or difficulty coordinating from interagency partners due to competing priorities and limited bandwidth. To mitigate these risks, CDP will strengthen and streamline communication and coordination mechanisms with the Interagency, establish regular meetings, and lead the development of a U.S. International Cyberspace and Digital Policy Strategy.

4. Bureau Cross-Cutting Management Goal

Bureau Cross-Cutting Management Goal 1: Create a positive, career-enhancing place to work, with clear processes and a cohesive bureau culture that values innovation and collaboration.

- **Bureau Cross-Cutting Management Goal 1 Description:** CDP will employ a multifaceted approach that considers the needs of employees, CDP's goals, and the demands of our operating environment to create a positive, career-enhancing workplace. Having clear and well-defined processes can help employees understand their roles and responsibilities, minimize confusion, and increase efficiency. Valuing innovation will encourage employees to think beyond the status quo, take risks, and be creative. Fostering a culture of collaboration is essential for the development of an innovative and cohesive culture.

CDP also seeks to promote career growth and development by providing employees with opportunities for training, mentoring, and career advancement, as well as recognizing and rewarding employees for their achievements and contributions.

Bureau Cross-Cutting Management Objective 1.1: Hire, develop, and retain a diverse and highly qualified workforce.

- **Bureau Cross-Cutting Management Objective 1.1 Justification and Linkages:** As a new bureau, CDP faces the challenge of attracting and retaining a diverse and highly qualified workforce that can enable its future success. Current staffing is well below planned levels, and the bureau is focused on filling vacant billets with strong candidates that can help us achieve our mission.

This objective aligns to JSP Goal 4 – Revitalize the diplomatic and development workforce and institutions.

- **Bureau Cross-Cutting Management Objective 1.1 Risk Considerations:** The risks associated with this objective include the fierce competition for talent, especially for candidates with specialized skills in areas such as cybersecurity and digital policy. The cumbersome and slow nature of our hiring practices and procedures also presents a risk. To mitigate these risks, CDP will seek to utilize its flexible hiring authorities, closely coordinate with GTM and others across the Department to streamline hiring processes, and develop recruiting and retention programs that address CDP's unique challenges.

Bureau Cross-Cutting Management Objective 1.2: Establish, implement, and strengthen CDP processes and systems to maximize effectiveness and efficiency.

- **Bureau Cross-Cutting Management Objective 1.2 Justification and Linkages:** As a new bureau, CDP has the opportunity to develop new processes and procedures that allow it to effectively and efficiently accomplish its mission. The establishment and implementation of strong processes and systems will lead to higher quality products and services across the bureau and increased customer satisfaction.

This objective aligns to JSP Goal 4 – Revitalize the diplomatic and development workforce and institutions.

- **Bureau Cross-Cutting Management Objective 1.2 Risk Considerations:** Without established process and procedures, CDP faces the risk of its people not understanding how to operate effectively and efficiently. To mitigate this risk, CDP will use inclusive processes to develop, update, and distribute bureau processes and SOPs for the provision of HR, IT, security, budget, and other services. In addition, CDP will work to communicate closely with all members of the CDP team to ensure they understand CDP processes and systems.

Bureau Cross-Cutting Management Objective 1.3: Cultivate a bureau culture grounded in diversity, equity, inclusion, accessibility, collaboration, and innovation.

- **Bureau Cross-Cutting Management Objective 1.3 Justification and Linkages:** Diversity in the workplace can provide numerous benefits, including increased creativity, better problem-solving, and a broader range of perspectives. CDP seeks to establish a diverse and inclusive culture across the bureau by creating an environment where everyone feels valued and respected, regardless of their background, race, gender, or any other personal characteristic. In addition, the bureau seeks to develop a culture that is focused on collaboration and innovation given that these attributes will be paramount to our success.

This objective aligns with JSP Strategic Objective 4.1: Build and equip a diverse, inclusive, resilient, and dynamic workforce.

- **Bureau Cross-Cutting Management Objective 1.3 Risk Considerations:** CDP, like other bureaus, faces the risk of not being able to effectively engage its entire workforce and realize the benefits of diverse, collaborative, and innovative thinking. To mitigate this risk, CDP is utilizing a Diversity, Equity, Inclusion, and Accessibility (DEIA) Council and tasking it with developing a plan for addressing DEIA related challenges. CDP is also developing a set of organizational values that emphasize attributes, actions, and characteristics that are important to the bureau.